UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,650	12/20/2001	Anton C. Rothwell	NAI1P056/01.187.01	2721

28875 7590 07/28/2008

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CHEA, PHILIP J	

ART UNIT	PAPER NUMBER
2153	

MAIL DATE	DELIVERY MODE
07/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/028,650	ROTHWELL ET AL.	
	Examiner	Art Unit	
	PHILIP J. CHEA	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-7,9,12-14,16-20,22,25-31,33-41 and 43-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7,9,12-14,16-20,22,25-31,33-41 and 43-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to an Amendment filed May 27, 2008. Claims 1,3-7,9,12-14,16-20,22,25-31,33-41,43-46 are currently pending, of which claims 44-46 are new. Any rejection not set forth below has been overcome by the current Amendment.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1,3,4,7,12-14,16-17,20,25-31,34,38-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan et al. (US 6,075,863), and further in view of Chi (6,006,329), and further in view of Lerche et al. (US 5,511,163), herein referred to as Lerche.

As per claim 1, Krishnan discloses a network adapter system, comprising:

a processor positioned on a network adapter coupled between an end-point computer and a network (see column 2, lines 33-39, where network adapter is considered the software-controlled modem), the network adapter capable of being installed on the end-point computer (see column 2, lines 44-50);

wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses (see column 5, lines 16-28, where processor executes applets to scan incoming data such as hazardous programs and viruses and content is considered “junk e-mail”);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses).

Although the system disclosed by Krishnan shows substantial features of the claimed invention (discussed above), it fails to disclose that the virus scanning utilizes virus signature files and that the virus signature files are stored on non-volatile solid state memory on the network adapter.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan, as evidenced by Chi.

In an analogous art, Chi discloses scanning data streams for viruses (see Abstract) using virus signature files to detect known viruses (see column 3, lines 47-65).

Given the teaching of Chi, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan by employing virus signatures, such as disclosed by Chi, in order to detect the viruses without having to store the entire virus code.

In considering the virus signature files being stored on non-volatile solid state memory on the network adapter, Krishnan shows storing virus detection applets and program code implementing a virtual machine for execution of programs in ROM and battery backed RAM for long term storage (see column 2, line 65 – column 3, line 12). Therefore it would be obvious to also store the virus signature files with the applets and program code in order for the applets executing the virus scan to use the signatures to detect viruses.

Although the system disclosed by Krishnan in view of Chi shows substantial features of the claimed invention (discussed above), it fails to disclose that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi as evidenced by Lerche.

In an analogous art, Lerche discloses a system with a computer and a network adapter that is able to receive all information on the network and the adapter can perform an assembling and scanning of all files on the network and carry out a recognition of virus signatures (see Abstract). Lerche also discloses that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter (see column 1, lines 38-49, *showing that a predetermined amount of packets (i.e. amount of packets making up the one file that is scanned) are assembled into one file and then determined if they are of interest by scanning them for detection of virae and the packets are received at a network adapter in order to intercept the packets and scan them*).

Given the teaching of Lerche, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi by employing assembling of the received packets, such as disclosed by Lerche, in order to catch all potential viruses on a network of computers.

As per claims 3,16, Krishnan discloses that the processor is capable of being user-configured locally (see column 3, lines 24-26)

As per claims 4,17, Krishnan further discloses that the processor is capable of being user-configured remotely via a network connection with the network adapter (see column 3, lines 36-37).

As per claims 7,20, Krishnan further discloses that the settings of the network adapter are capable of being user-configured (see column 5, lines 33-35).

As per claims 12,25, Krishnan further discloses that the processor is capable of denying received packets that fail the scan (see column 5, lines 16-23).

As per claims 13,26, Krishnan further discloses that the scan is performed based on user settings (see column 3, lines 2-6).

As per claims 14,27,28, Krishnan in view of Chi in view of Lerche disclose a method for scanning network traffic on a network adapter, comprising:

receiving packets at a network adapter including a processor positioned thereon, the network adapter being capable of being installed on an end-point computer (see Krishnan column 2, lines 33-39, where network adapter is considered the software-controlled modem);

virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses (see Krishnan column 5, lines 16-28, where processor executes applets to scan incoming data and content is considered “junk e-mail”); and

conditionally taking security measures if the packets fail the scan (see Krishnan column 5, lines 16-23);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses);

wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter (see Lerche column 1, lines 38-49).

As per claim 29, Krishnan in view of Chi in view of Lerche disclose a network adapter system, comprising:

a processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module (see column 2, lines 56-65, where it is implied if not inherent that there is a packet assembly module in order to receive data from the outside see column 5, lines 16-18 for scanner module);

a user interface driver for identifying network traffic of interest transmitted between the computer and the network (see Krishnan column 5, lines 24-31);

wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the computer and the network (see Krishnan column 5, lines 16-31);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

wherein the network adapter receives the network traffic (see Krishnan column 5, lines 16-23);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses);

wherein a predetermined amount of the received network traffic is assembled for determining whether the received network traffic is of interest, the received network traffic including network traffic received at the network adapter (see Lerche column 1, lines 38-49).

As per claim 30, Krishnan further discloses that the content scanning enforces operational policies of an organization (see column 5, lines 24-30).

As per claims 31,40, Krishnan further discloses that the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation (see column 5, lines 24-30).

As per claim 34, Krishnan further discloses that the packets that are of interest include executable files (see column 5, lines 16-23).

As per claim 38, Krishnan further discloses that the network adapter includes a cable modem adapter (see column 6, lines 36-45).

As per claim 39, Krishnan further discloses that the network adapter includes a broadband adapter (i.e. cable modem).

3. Claims 5,18,33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claims 1,14 above, and further in view of Bonomo et al. (US 6,658,562), herein referred to as Bonomo.

As per claims 5,18,33, although the system disclosed by Krishnan in view of Chi shows substantial features of the claimed invention (discussed above), it fails to disclose that memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Bonomo.

In an analogous art, Bonomo discloses a system for setting different BIOS configurations stored in a memory device (see Abstract). Further showing setting a password to view information in a BIOS setup program or to change configuration (see column 4, lines 11-21 and 30-41).

Given the teaching of Bonomo, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing a password protected BIOS, such as disclosed by Bonomo, in order to prevent unwanted users from changing settings without authorization.

4. Claims 6,19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claim 1 above, and further in view of Templeton (US 6,401,210).

Although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose that the manner in which the scanning performed is user-configured.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Templeton.

In an analogous art, Templeton discloses a system for managing files infected by computer viruses (see Abstract). Further disclosing that the manner in which the scanning performed is user configured (see column 4, lines 8-35, describing scan options that are user configured).

Given the teaching of Templeton, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing user configured scan options, such as disclosed by Templeton, in order to perform specific actions when a virus is detected.

5. Claims 9,22,43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claims 1,14 above, and further in view of Makinson et al. (US 7,023,861), herein referred to as Makinson.

As per claims 9,22, although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose that the packets of interest are based on an associated protocol.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Makinson.

In an analogous art, Makinson discloses a bridge with a built in scanner connected to an end-user computer (see Fig. 5), where the scanning of packets may be selected based on the certain types of protocols (see column 4, lines 50-57).

Given the teaching of Makinson, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing protocol specific scanning, such as disclosed by Makinson, in order to relieve the processor from scanning unnecessary packets.

As per claim 43, Makinson further discloses that the received packets that are not of interest to the end-point computer bypass the scanning (see column 4, lines 50-57).

6. Claims 35-36, are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche.

As per claim 35,36, Krishnan in view of Chi in view of Lerche does not expressly disclose that the network adapter includes a Peripheral Component Interconnect (PCI) card and/or an Industry Standard Architecture (ISA) card. However, Krishnan does disclose that the adapter can be an add-in card for installation in an expansion slot of a computer comprising an expansion bus interface (see column 2, lines 47-50). At the time of the invention, a person having ordinary skill in the art would have recognized that PCI and ISA are commonly used and well known expansion bus interfaces. Therefore it would have been obvious to make network adapters for both PCI and ISA in order to provide an adapter compatible with most computers.

7. Claims 35-37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claim 1 above, and further in view of Sridhar et al. (US 5,799,064), herein referred to as Sridhar.

As per claims 35,36 although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose that the network adapter includes a Peripheral Component Interconnect (PCI) card and/or an Industry Standard Architecture (ISA) card.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Sridhar.

In an analogous art, Sridhar discloses an apparatus interfacing between a communication channel and a processor for data transmission and reception (see Abstract) further showing that the apparatus may be connected to a bus such as an ISA or PCI bus (see column 3, line 63 – column 4, line 2).

Given the teaching of Sridhar, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing a network adapter including a PCI and/or ISA card, such as disclosed by Chi, in order to connect to the bus of the end-point computer.

As per claim 37, Sridhar further discloses that the network adapter includes an Integrated Services Digital Network (ISDN) adapter (see column 4, lines 11-19).

8. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claim 1 above, and further in view of Horvitz et al. (US 6,161,130), herein referred to as Horvitz..

Although the system disclosed by Krishnan shows unwanted content includes junk e-mails and misinformation (see column 5, lines 24-25 for junk e-mail and column 5, lines 16-18, where Trojan horses are considered misinformation), it fails to disclose harassing content and pornographic content.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Horvitz.

In an analogous art, Horvitz discloses a system that detects electronic mail messages that the recipient is likely to consider junk (see Abstract). Further disclosing that the unwanted messages include harassing content and pornographic content (see column 9, lines 44-51, where harassing content is considered abusive or insulting messages).

Given the teaching of Horvitz, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing a harassing content and pornographic content filter, such as disclosed by Horvitz, in order to keep the incoming data safe for users.

9. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claim 29 above, and further in view of Maher, III et al. (US 6,910,134), herein referred to as Maher.

Although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose that the packet assembly module utilizes header information associated with received packets for assembling data fields of the received packets.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Maher.

In an analogous art, Maher discloses a system for detecting and inoculating email infected with viruses (see Abstract). Maher goes into further detail about a packet assembly module to reassemble data packet fragments and how the header information is utilized to assemble the packets (see column 4, lines 47-59).

Given the teaching of Maher, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by

employing a header pre-processor to assemble data fields of the received packets, such as disclosed by Maher, in order to scan the payload for known virus signatures.

10. Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claim 1 above, and further in view of Hursey et al. (US 7,107,617), herein referred to as Hursey.

Krishnan discloses that received packets that are of interest fail the scanning (see Krishnan column 5, lines 16-23).

Although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose that if the received packets that are interest fail the scanning, an alert is displayed which provides remedy options.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Hursey.

In an analogous art, Hursey discloses a malware scanner to compare malware signatures to files (see Abstract). Hursey further discloses that if a virus signature has a match, anti-virus actions are triggered which may include deletion, quarantine, repair, alert message generation, etc.

Given the teaching of Hursey, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing remedy options, such as disclosed by Hursey, in order to aid in a fix for the infected computer.

11. Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche as applied to claim 1 above, and further in view of Edwards et al. (US 7,188,367), herein referred to as Edwards.

Although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose scanning the received packets that are of interest is prioritized based on a file type associated with the received packets.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by Edwards.

In an analogous art, Edwards discloses a virus scanner with a pre-processor that gathers characteristics about the scan the scan request and places them in a queue. Edwards further discloses that the certain file types can be given priority over other file types (see column 6, lines 17-22).

Given the teaching of Edwards, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing prioritized file type scanning, such as disclosed by Edwards, since in some server environments it might be determined that ensuring quick access to executable files increases the usability of the system (see Edwards column 6, lines 20-22).

Response to Arguments

12. Applicant's arguments filed May 27, 2008 have been fully considered but they are not persuasive.

A) Applicant contends that Lerche does not disclose a predetermined amount of the received packets are assembled for determining whether the received packets are of interest.

In considering A), the Examiner respectfully disagrees. Lerche discloses assembling a predetermined number of packets because the number of packets that make up one single file is predetermined. Once the one file is assembled, the packets are scanned for virae (see column 1, lines 38-50). The claim does not clearly mention that the predetermined number can't be all of the packets circulating the network. Therefore, the cited reference meets the claimed limitation since it is predetermined that the number of packets are all packets received by the network. Furthermore, the received packets are being assembled because a network adapter receives the packets before they are scanned (see column 1, lines 38-50). Applicant also contends that Lerche does not discloses that the processor determines whether the received packets are of

interest. However, Lerche was merely used to teach the assembly of a predetermined number of packets. Krishnan was used to teach that a processor determines whether received packets are of interest in column 5, lines 16-23.

B) Applicant contends that Lerche does not disclose that the manner in which the scanning is performed is user-configured.

In considering B), the Examiner believes that updating applets which can effect the scanning of Trojans and worms, etc. implies the user-configured manner of scanning. That is if a new applet is installed which has an updated virus detection program, the manner of scanning has changed (see Krishnan column 5, lines 16-28, showing how different applets can scan for different things such as viruses, worms or Trojans or scan for junk e-mail). However, for clarity, the Examiner has introduce a new reference Templeton which is believed to clearly teach this limitation.

C) Applicant contends that Krishnan fails to disclose enforcing operational policies of an organization.

In considering C), the Examiner respectfully disagrees. It is noted that in the specification, operational policies of an organization can be detecting harassing or pornographic content, junk e-mails, viruses, etc. (see Specification page 9, lines 7-10). Krishnan shows an applet providing filtering of junk e-mail and other unwanted data (see column 5, lines 25-30) and scanning for viruses (see column 5, lines 16-20). Since Krishnan shows that junk e-mail is filtered, the organizational policy of junk e-mail would be enforced. It is believed that this teaching is enough evidence to support the enforcement of operational policies.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHILIP J. CHEA whose telephone number is (571)272-3951. The examiner can normally be reached on M-F 6:30-4:00 (1st Friday Off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Philip J Chea
Examiner
Art Unit 2153

PJC 7/23/08
/John Follansbee/
Supervisory Patent Examiner, Art Unit 2151